Information Polity 28 (2023) 43–59
DOI 10.3233/IP-211508
IOS Press

The role of trust in the adoption of cooperative arrangement types in e-credentials markets

Ali A. Guenduez[a,*], Tobias Mettler[b] and Kuno Schedler[a]
[a]*Smart Government Lab, University of St. Gallen, St. Gallen, Switzerland*
[b]*Swiss Graduate School of Public Administration (IDHEAP), University of Lausanne, Lausanne, Switzerland*

Abstract. The interest in digital identities has increased considerably in academia and practice in recent years. This can be seen by the many electronic identity projects worldwide and the numerous published studies that provide insightful narratives and descriptive case findings about success factors and barriers to the adoption of national authentication infrastructures. In this paper, we take a closer look to the role of trust on the design and implementation of a nation-wide e-credential market. We argue that trust in political and economic institutions can be an important factor to explain differences in the chosen cooperative arrangement which can range from monopolistic, purely state-controlled e-credential markets, to polypolistic, decentralized e-credential markets where also private vendors offer state recognized e-ID on their own or in partnership with the government. Following an inductive reasoning process, we develop three testable propositions which may inspire further empirical research and offer practitioners a new angle to rethink e-credential markets in the light of citizen trust in political and economic institutions.

Keywords: Digital identity, e-credential markets, state-recognized digital identity, theory development, trust

Key points for practitioners:

- Electronic identities are becoming a cornerstone of digital government infrastructure.
- Different cooperative arrangements are possible for developing an e-credentials market.
- Trust in technology, politics, and the economy are decisive factors for choosing options.
- We develop theoretical propositions that link trust to the design of e-credentials markets.

1. Introduction

Enabling and strengthening secure and trustworthy identification in online interactions has become an ongoing challenge for both governments and economies. Traditional identification via paper-based documents or physical appearance seldom fits today's virtual world of the Internet (Whitley et al., 2014). Thus, there is an urgent need for a functional equivalent of paper-based identification for the digital sphere that, like traditional identity cards or passports, captures the characteristics of a person or organization and distinguishes them from others. In light of this development, electronic identification (e-ID) has become

*Corresponding author: Ali A. Guenduez, Smart Government Lab, University of St. Gallen, Dufourstrasse 40a, 9000 St. Gallen, Switzerland. E-mail: aliasker.guenduez@unisg.ch.

critical for e-government and e-commerce alike in order to foster safe online relationships (Wihlborg, 2013).

e-ID fulfills two primary purposes: identification and authentication. *Identification* refers to the process necessary to perform a unique verification or determination of the identity of a person (or organization) by showing, referencing, or letting a third party know who someone (or something) is (Strauss, 2011). *Authentication* refers to the proof of genuine nature of a declaration of intent or act in the sense that the purported source of a statement or act is in fact who it claims to be (Lentner & Parycek, 2016). e-ID provides the unique identity of a person by generating and linking to a set of identifiers that can clearly distinguish a person from all others and can consist of name, address, mobile phone number, social security number, password, or electronic signature derived from a national register (Graux et al., 2009). Physically stored in an encrypted form on an e-ID medium, such as a USB stick or a mobile phone's SIM card (Lentner & Parycek, 2016), e-ID becomes portable – like any paper-based identification object. Most e-ID systems use smart card technology, which allows one to combine possession (e.g. a material thing) and knowledge (e.g. a PIN code). This provides a higher security level than purely knowledge-based systems, which do not rely on a physical device.

Besides the research into e-ID's technological features, a constant yet peripheral stream in the digital government literature has dealt with the design and organization of e-credentials markets and the state's role(s) in doing so (Arora, 2008; Eaton et al., 2018). While these studies provide insightful narratives and descriptive case findings about the success factors and the barriers to the adoption of national e-ID infrastructures (Bostan et al., 2017; Cordella & Paletti, 2019; Grönlund, 2010; Hornung & Rossnagel, 2010; Mir et al., 2019; Rissanen, 2010), there has been very little theorizing about possible determinants for or against a publicly or a privately driven e-credentials market. A better understanding of the factors that influence the prevalence of purely governmental, purely private, or mixed solutions in e-credentials markets can help us to better understand the adoption and focus of the various solutions. We seek to contribute to this and to provide new insights by focusing on trust's role in the adoption of cooperative arrangements in e-credentials markets.

Scholars agree that trust is a crucial enabling factor in relationships where there is uncertainty or risks (Rousseau et al., 1998; Simpson, 2007), which is the case in online transactions and interactions (Friedman et al., 2000). Despite significant research into trust's role in the adoption of e-government (Belanger & Carter, 2008; Lee et al., 2011), analyses on its role in e-credentials markets have, with exceptions (Seltsikas & O'Keefe, 2010), scarcely been researched. We explore the relationship between trust and the adoption of cooperative arrangements in national e-credentials markets, focusing on trust in the political and the economic institutions, defined as the confidence people have in these institutions that they are generally dependable and can be relied on (Luhmann, 1979). With this research goal in mind, we ask:

> *What role does trust have in the choice of the adoption of cooperative arrangements in e-credentials markets?*

To answer this research question, we analyzed various data sources. We began our analysis by reviewing pertinent documents and the literature, and then deepened our findings through interviews with experts involved in e-ID projects in various European countries, including the UK, Belgium, the Netherlands, Germany, Hungary, Austria, and Switzerland. These are very similar e-ID markets, since for instance eIDAS (EU regulation on electronic identification and trust services) plays an important role in all European countries. However, they differ in whether the e-IDs are issued by private or public entities and/or in public-private partnerships (PPPs), making them suitable to gain insights into trust's role in the adoption of cooperative arrangements.

We will now develop theoretical propositions linking trust to the design of e-credentials markets based on an inductive reasoning process. After analyzing the extant research, we started the theory development by delineating constructs and their interrelationships in the form of theoretical propositions. We then mapped several European e-ID initiatives to identify a certain pattern. We conclude with a discussion on our work's implications and provide suggestions for research and practice.

2. Background

In this section, we use the literature to conceptualize the phenomenon and to develop our theoretical propositions. The theory development process was further guided by the building blocks defined by Dubin (1978) and Whetten (1989). We start by delineating possible cooperative arrangements of how to organize an e-credentials market and then turn to the explanation of trust's role in building such a critical information infrastructure.

2.1. Different actors, and cooperative arrangements in a state-recognized e-credentials market

In short, e-ID is about providing services in a secure, efficient, and trustworthy way, for public administration as well as for citizens and businesses (Melin et al., 2016; Strauss, 2011). A key security concern is to reduce online fraud, i.e. to combat identity theft and thereby enable secure online communications and transactions. e-ID is considered to be a strong, secure technology for online authentication. It can reduce fraudulent activity on the Internet by ensuring that the online (legal or natural) person is in fact who they claim to be. This is particularly relevant in areas where citizens are expected to provide detailed personal information (Seltsikas & O'Keefe, 2010). It prevents the misuse of personal data and creates transparency regarding access to personal data (Hornung & Rossnagel, 2010). An additional advantage of a national e-ID solution is the increased process integration it offers concerning government applications. e-ID-based services are also expected to increase convenience of usage. Citizens will be able to use a wide range of electronic services at any time of the day and from any geographical location. This gives online users access to a much wider range of electronic services that are offered in an integrated way. The increased availability and convenience of e-ID-based services is expected to positively impact on user satisfaction with electronic services (Seltsikas & O'Keefe, 2010). Further, not only at national but also at supranational level, e-ID can help address identity fraud and can establish e-services that go beyond national borders (Arora, 2008). In Europe, for instance, e-ID is seen as a key tool for the provision of e-services and the detection and tracing of fraud transnationally. The ability to interact and communicate with different governmental agencies, even across national borders, is seen as an important prerequisite for digital transformation and the creation of a digital single market (Gomes de Andrade et al., 2013).

Today, there are different cooperative arrangements in place for e-ID issuance and the maintenance of a national e-ID infrastructure, all with the aim of exploiting the different opportunities offered by e-ID and keeping potential threats under control. A national (or cross-border) e-ID infrastructure may vary in terms of the technical architecture, institutional actors involved, and the range of services that can be accessed by citizens using digital identities (Spagnoletti et al., 2019). Before explaining the different arrangements on how to organize an e-credentials market, we will first briefly define who the key actors are (see Fig. 1).

Identity providers (IdPs) are the entities that are responsible for issuing e-ID. This is generally a government agency or a trusted third party. They develop and maintain the technical infrastructure required for the authentication and identification of citizens, ensure the infrastructure's security and operational reliability, assign and manage personal requests for e-IDs, store user account and profile

Table 1
Different cooperative arrangement types in e-credentials markets

Arrangement	Definition	Examples
Public	The government is primarily responsible for the development, implementation, management, and maintenance of e-ID.	DigiD (the Netherlands), elektronische Personalausweis (Germany), DNIe card (Spain), beID (Belgium)
Private	One or more private vendors are responsible for the development, implementation, management, and maintenance of e-ID. Government provides proof of citizens' credentials, and accredits and controls e-ID providers and their systems.	BankID (Sweden), Buypass (Norway), Itsme (Belgium)
PPP	Both the government and one or more private companies are responsible for the development, implementation, management, and maintenance of e-ID.	Bürgerkarte (Austria), NemID and MitID (Denmark), Idensys (the Netherlands)

information, and bear the responsibility and liability for the authenticity and validity of identities (Arora, 2008; Mettler & Guenduez, 2019).

Certification authority: Depending on the cooperation arrangement, the state may refrain from issuing e-IDs, focusing instead on the regulation of the e-credentials market and the certification of third parties. This may include the definition of a coherent and applicable legal framework, quality control, and the sanctioning of misconduct by actors involved in the e-credentials market. However, certification may also be done by another private firm on behalf of the state. IdPs that comply with the defined standards and regulations regarding security, data protection, and interoperability may then receive a certificate and are then entitled to call themselves a preferred or a state-recognized IdP.

Online service providers – also called *relying parties* – can be private companies or government agencies that offer digital services such as e-banking or electronic medical records for which they require reliable proof of a citizen's identity. Online service providers offer services to users with an e-ID from an official identity provider with whom they have an agreement. When providing online services, they rely on IdPs for user authentication.

Users: Citizens who meet the requirements (usually a valid identity card or minimum age) can obtain an e-ID, thereby becoming identity owners. As owner of an e-ID, citizens have mainly two touchpoints with other actors: with the OsP from which they request digital services and with the e-ID provider to define which information to share with which OsP.

Depending on the role(s) a government wants to play, we see three generic organizational arrangements of a state-recognized e-credentials market, as shown in Table 1.

The characteristic feature of a *public* e-credentials market is that e-ID issuance is centralized and managed by the state. Here, the government has multiples roles. The government is on the one hand responsible for the development, implementation, management, and maintenance of the e-ID. It is the certifier, identity provider, and service provider, all at the same time. In its role as a regulatory authority, the government lays down the rules and procedures to which it is subject as a provider when issuing, managing the e-IDs and providing related services to users. The objectives of such a solution often relate to e-government services, where e-ID builds on existing identity verification tools and extends or adapts them to the online world (Muñoz-Cañavate & Hípola, 2011). e-ID is seen as part of a wider program aimed at improving and modernizing the government services. Thus, the primary objective of implementing e-ID is to improve the delivery of public services to citizens and businesses. The business model for a state e-ID is simple. Citizens have little or no financial obligations because government subsidizes e-ID implementation.

In a *fully private but government-approved e-ID*, government outsources e-ID provision to private sector vendors, recognizing and certifying them for this service. The responsibility for the implementation,

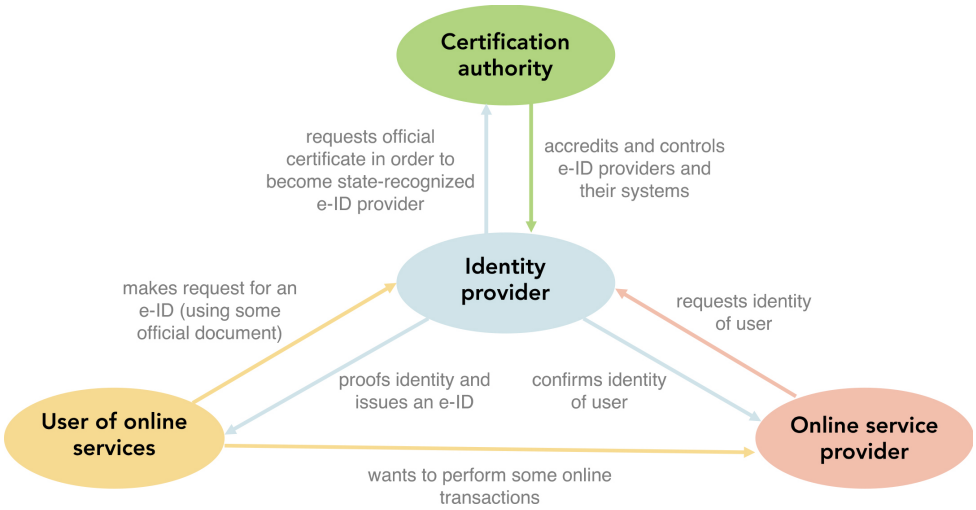

Fig. 1. Actors and activities in a state-recognized e-credentials market.

maintenance, and control of e-ID lies with the certified companies. They act as IdPs under the supervision of governmental actors. The IdPs must guarantee the identification and authentication of citizens and must securely manage their personal data and enable access to services offered by public and private service providers (Spagnoletti et al., 2019). The government therefore focuses primarily on certifying e-ID providers as suppliers of state-recognized identity information and regulating the market, while private identity providers use the digital environment to develop new and innovative revenue sources. Moreover, e-ID issued by private vendors, provide access to both public and private services such as for storing health insurance information. However, typically these e-ID integrate private services of their relying partners. The business model relies on the payments of the *online service providers*, which are charged a transaction fee by the IdP that manages the citizens' identities and that performs the authentication. Citizens may also have to pay fees for additional services (e-signature, higher security levels, etc.). The state becomes a trusted third party and pays the fees for the provision of e-government services. Nonetheless, in this model, the implementation of e-ID is considered to be more cost-effective than a state-centered model, because large investments by the government are avoided (Grönlund, 2010).

In the case of a *PPP*, government authorities work with one or more private companies in issuing e-ID. While private vendors are often involved in developing e-ID and infrastructure, the state retains strong control over the e-credentials market. The PPP aims to make both services accessible electronically with a single e-ID and also strives to reduce costs and make e-government services available to more citizens, thereby meeting the national e-government strategy's objectives. e-ID also enables access to services offered by private businesses, such as logging into bank, insurance, or health accounts. The PPP business model depends on cooperation between private companies and the government. Generally, the less the state is involved, the fewer costs it bears. Depending on the specific arrangements, the costs are also passed on to private companies and/or to customers.

Irrespective of the cooperative arrangements of e-credentials markets, the creation of national e-ID systems is associated with far-reaching changes that concern technological, legal, political, and organizational aspects. In this sense, e-ID is more than a technology for identifying citizens and organizations; it affects the core of citizenship. It is therefore becoming a political issue (Strauss, 2011). Closely related to this is the question whether the state or private vendors should provide e-ID. We will now look at the

role of trust, which we believe helps one to understand why some governments issue e-ID in-house and others contract it out to private vendors. To this end, we will now consider trust in technology, trust in the government, and trust in the economy.

2.2. Trust's role in e-credentials markets

Trust is a complex construct that is hard to define and even harder to measure (Simpson, 2007). It has received widespread theoretical and empirical studies, but has remained an elusive concept that has been conceptualized and used in very divergent ways (McKnight & Chervany, 1996). However, trust is a crucial component of any social interaction, whether offline or online (Friedman et al., 2000; Wang & Emurian, 2005). It influences how a person copes with their social context (McKnight et al., 2002). It fundamentally affects a person's interaction with their social environment (Rousseau et al., 1998). This also applies to interactions in the digital sphere, particularly because the risk of cyberattacks on critical information infrastructures is omnipresent (Alcaraz & Zeadally, 2015). National e-ID systems are as vulnerable to attacks as any other IT infrastructure. Besides security concerns, the technical requirements for e-ID are already in place, but the social aspects for developing trust lag behind. In some countries, the required legal framework for implementing e-ID is not yet in place. Efforts to harmonize national regulations are also still needed (Wihlborg, 2013). Further, human error, which can occur at any stage of interaction with a system, is a further threat to the e-credentials market. Even the simplest mistake, such as entering incorrect data during registration, can jeopardize e-ID usage (Arora, 2008). Further challenges to e-ID adoption relate to the lack of intergovernmental coordination, the lack of private-public sector cooperation, and tensions such as the tradeoff between usability and security. Also, privacy concerns and related demands to enhance transparency and enable citizens to effectively control their personal data are major challenges faced by governments (Melin et al., 2016; Spagnoletti et al., 2019; Strauss, 2011).

Thus, we distinguish between three key aspects of trust that may influence e-credentials markets, namely trust in a government, trust in economic institutions, and trust in technology.

Trust in a government is often conceptualized as whether or not the political authorities and institutions operate in accordance with citizens' normative expectations (Grimmelikhuijsen et al., 2013). Trust in government relates closely to whether citizens perceive and judge a government's actions as honest, efficient, right, and fair. Thus, trust in a government is a key indicator of citizens' satisfaction with a state's policies and whether its related actions are perceived as legitimate (Blind, 2006; Cheema, 2010; Tolbert & Mossberger, 2006). The credibility and transparency of a government, its services and institutions, and the behaviors of its public officials strongly influence whether or not citizens trust their government (Cheema, 2010; Grimmelikhuijsen et al., 2013). Trust is often seen as a cause of or a correlate for various behaviors that directly or indirectly impact on policy outcomes (Llewellyn et al., 2013). For instance, low trust is therefore associated with low political participation (Putnam, 1993). Trust's role is particularly evident in the implementation of e-government projects. A lack of trust for instance in a government's ability to implement appropriate programs can result in citizens becoming unwilling to accept the corresponding services (Morgeson et al., 2011; Seltsikas & O'Keefe, 2010). A lack of trust also may lead to opportunistic behaviors and may contribute to 'free-riding' behavior (Cheema, 2010). Thus, some studies have focused on how trust in organizations can be repaired and enhanced (Kramer & Lewicki, 2010): In order for citizens to support e-government initiatives, they need to be convinced that government authorities have the expertise and the technical skills to implement and secure such projects (Belanger & Carter, 2008).

Trust in economic institutions is critical, for several reasons. Trust in the economic system is particularly important, because a good economic situation increases the security of people and their businesses, promoting growth and economic prosperity (Enste & Grunewald, 2017). Such trust in economic institutions

is necessary to strengthen investor and consumer confidence and is crucial for economic activities (OECD, 2019). It also plays a decisive role concerning stability. Cross-country studies have shown that economic trust is negatively linked to macroeconomic instability. Higher confidence reduces the frequency of crises. Further, trust in the economy also reduces the volatility of investment but not of public expenditure, suggesting that it is likely a key factor for macroeconomic stability (Sangnier, 2013). Notably, trust in a government and trust in the economy are interrelated. People trust governments and their institutions that spur economic growth, create jobs, provide access to education, and deliver services in a simple and transparent way (Blind, 2006; Cheema, 2010).

Finally, *trust in technology* exists when "a user depends on the technology for an outcome, with the expectation that the hoped-for outcome come true, but the possibility exists that the technology may not enable that outcome." (Lankton et al., 2016). To date, while the relationship between trust and technology has been the subject of many studies (Hengstler et al., 2016; Komiak & Benbasat, 2006; Lee et al., 2011; Luo et al., 2010; Sicari et al., 2015), there are still no consistent findings across the different research fields. This also applies to research into technology adoption in the public sector. Studies on e-government services have found that willingness to adopt e-government services does not depend only on trust in technology, but significantly, rather on trust in the institution that delivers these services (Teo et al., 2008; Welch et al., 2005). However, other studies suggest that trust in technology also plays an important role in e-government adoption (Carter & Belanger, 2005).

3. Theory development

In this section, we develop our hypotheses based on an inductive reasoning process. Our hypotheses take the form of testable propositions, as we followed the logic proposed by Popper (1934), who understood theorizing in part as the specification of universal statements that can be verified against observations of what occurs in the real world. We will do this at the end of this section.

3.1. Inductive approach

To develop our hypotheses, we decided to use an inductive, data-driven qualitative research approach. An inductive approach involves "using detailed readings of raw data to derive concepts, themes, or models through interpretations made from the data by researchers." (Thomas, 2006, p. 238). The generation of theoretical statements draws on the wealth of information available in the data. Our research strategy can best be described as a sequential *qual-qual multimethods design* that allowed us to obtain different information types and to answer our research question more comprehensively (Morse, 2010).

Our starting point was a review of the literature concerning e-ID studies. We followed Webster and Watson's (2002) methodology for a systematic literature review. We sought to identify patterns, themes, and issues and to thereby gain an understanding of how the literature addresses e-ID, e-credentials markets, and trust. When searching and reviewing the literature, we not only focused on the public administration discipline, but also on interdisciplinary studies. We used *Web of Science* as the database for the literature search. We identified research articles on e-ID in three search steps: (1) initial search, (2) main search, and (3) a forward and backward search. The initial search was used to define the search criteria to be used in the primary search. During the initial search process, it turned out that we needed to apply multiple terms and other spellings for e-ID, such as 'electronic identity' or additional terms such as 'digital identity,' in order to obtain an appropriate article sample set. We refined our search in step 2, and obtained 264 research articles. We then manually filtered by further examining each article's abstract

Table 2
Sample documents used

#	Document type	URL
1	Digital Government Factsheets of the European Commission	https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-government-factsheets
2	Documentation of the Italian Ministry of the Interior on National ID	https://www.cartaidentita.interno.gov.it
3	Belgian national identity card	https://eid.belgium.be/en
4	Documents on BankID in Sweden	https://www.bankid.com/bankid-i-dina-tjanster/rp-info#
5	e-ID report of the city of Zug in Switzerland	https://www.stadtzug.ch/digitaleid/5295
6	Documentation on NemID and MitID	https://en.digst.dk/digitisation/eid/
7	Documentation on Ireland's MyGovID	https://www.mygovid.ie/
8	Poland's national pl.ID	https://plid.obywatel.gov.pl/

and screening the article's content. We only included papers with a clear focus on e-ID that had been peer-reviewed in journals or conferences and that were published in English. In step 3, we reviewed the articles' references to obtain additional sources (backward search) and also reviewed sources that cited the key articles identified in the previous steps (forward search). At the end of this review process, 21 articles remained. We then proceeded with an inductive evaluation of the concepts and results in these articles. Concretely, we independently read the article to gain an overview over the academic field. We identified relevant sections of text that provided insights into the characteristics of e-credentials markets. We focused on understanding key characteristics of e-credentials markets. However, we were unable to collect all relevant characteristics of the e-reference markets mentioned in the literature. While some were discussed in detail, for others only limited information was available. Therefore, following Bowen (2009), we simultaneously conducted document analysis of the publicly available descriptions of the e-credentials markets we had identified in the literature. We searched the Internet for official documents that described the cooperation arrangements of the e-credentials markets in more detail and analyzed them. Analyzing these documents had two advantages. First, by studying the documents derived from the national e-ID websites or from supranational institutions such as the Digital Government Factsheets of the European Commission (see Table 2), we identified and analyzed further e-credentials systems that were not identified in the literature. Second, the information from these documents complemented the insights already obtained from the literature. Studying the e-ID reports also enabled us to gather the latest information on e-ID systems. This was particularly important, because the date of publication of numerous studies is far behind and the data were not up to date. We then analyzed the data obtained from the literature and official documents, focusing on e-credentials markets for which sufficient valid data were available. This resulted in a dataset of 14 e-credentials markets, the focus being limited to European countries. We read the literature and the documents several times. Our objective was to inductively identify broad emerging themes and to "determine if there are any systematic patterns among the data 'worthy' of further attention." (Sabherwal & King, 1991, p. 192). Table 2 includes a sample overview over the documents we used.

After analyzing the literature and the documents, we found two main concepts to be particularly important for e-credentials markets: *trust in political institutions and economic institutions* as well as *cooperative arrangement* of how the different actors in the e-credentials market are working together. The literature and the document analyses allowed us to get first insights into these concepts as well as to further classify and identify variables that explain the variations between e-credentials markets. In our research, for instance, this initial analysis led to a working hypothesis that in a country, the trust level in the economic and political institutions seems to have a key role in the choice of e-ID systems. To substantiate our assumptions and to enhance our understanding, we conducted interviews with government officials

Table 3
Sample statements from the interviews

Interviewees	N	Sample of statements on trust
Responsible for digital identity, e-Government, and digital public services	4	The regulatory tradition and the public's understanding of the state are perceived as important factors when implementing e-ID; in some countries, e-ID is a political decision with no room for private companies; in other countries, the states relies on private sector companies' experience. Gaining citizens' trust and goodwill is perceived as the most important thing in e-ID implementation. Uncertainties about how the state or private companies deal with citizens' data lead to skepticism and long discussions about e-ID.
IT service provider	1	Both for the state and for private providers, building a basis of trust is of great relevance for the introduction of an e-ID. Citizens' trust in the state and commercial enterprises such as banks and insurance companies affects whether they prefer to receive their e-ID from the government or from private companies.
Private e-ID provider	3	Achieving the trust of a critical mass is a key factor. If the parties involved in an e-ID ecosystem don't trust one another, then no deals will happen. Recognition by the state and the involvement of renowned companies create trust in a private e-ID among citizens.
Online service provider	4	As end-users are required to disclose their personal data, building trust is crucial for the introduction of e-ID, irrespective whether government or private companies issue it. The question whether e-ID should be issued by the state, private entities, or both is often an emotional issue, with little reasoning and rationality. It's about a sense of primal trust, or a lack thereof.

($n = 4$), an IT service provider ($n = 1$), private e-ID providers ($n = 3$) and online service providers ($n = 4$) from the UK, Belgium, the Netherlands, Germany, Hungary, Austria, and Switzerland that are managing e-ID projects. Table 3 includes a sample overview over the interviewees and samples of their thoughts on trust.

3.2. Theory constructs

Based on the analyses and the interactions with practitioners, we proceeded to define our theory constructs. The main units of any testable proposition – whether enumerative, associative, relational, statistical, or complex (Dubin, 1978) – are the constructs that help to describe the phenomena of interest in the theory. Our theory has two main constructs: cooperative arrangement and trust.

We defined *cooperative arrangement* as the implicit or explicit agreement between the state and other private or public service providers to collaborate with one another for the purpose of delivering and managing the services required for the digital identification and authentication of citizens in a way that it is equivalent to a paper-based procedure and that complies with the applicable privacy laws. This definition entails multiple implications and limitations of scope. First, many providers of online services (such as Facebook and Google) grant users access to their accounts via a user name and a password (the login credentials). These identities are both how citizens identify themselves to service providers and how service providers authenticate or verify that users are who they say they are. However, we concentrated on state-recognized e-ID. State-recognized means that a government agency acknowledges a person's real identity. This stands in contrast to the abovementioned example relating to common social media or online services where this usually doesn't take place. Anyone can create an account under a false name or can have multiple fictitious identities. Second, we acknowledge that different agreement types and divisions of labor between the state and third parties are possible. There may or may not be a legal basis or formalized structures in place that ensure the coordination and integration of services. We did

not specify any base requirements or maturity or capability level, which are needed for an e-credentials market to be optimal. Third, we were interested in digital-only identification and authentication services. Hybrid forms are conceivable, where for instance a citizen physically identifies themselves once at the counter of a trusted party (e.g. a bank or a telecommunications provider) and then gains access to certain online services.

By *trust*, we mean citizens' expectations that the state or an involved third party (e.g. an IdP or OsP) is capable of providing secure digital services and will not exploit any vulnerabilities inherent in the e-credentials market, such as those caused by a lack of governance, regulation, or improper maintenance and management of technology. As noted, our understanding of trust addresses both interpersonal characteristics (i.e. how citizens feel about technology) and an institutional perspective (i.e. how they perceive the trustworthiness of the state or the economy). Again, our definition implies implications and assumptions. First, we understand trust as a relational (and not an absolute) concept. At any point in time, citizens' expectations can change based on the actions of an actor in the e-credentials market, such as providing a better service experience, or the lifting or imposing of certain constraints to getting access to e-ID services. Accordingly, what the state does or fails to do (consciously and/or unconsciously) influences how citizens assess the trustworthiness of the other stakeholders in an e-credentials market. The same applies to private service providers. Second, trust exists in an environment of mutuality, i.e. it is both time-bound and situation-specific. Inherent in many analyses of trust is the belief in an innate level of trustworthiness that may be shared among several like-minded persons or large parts of society in a specific situation (e.g. after a specific incident or crisis, such as a pandemic). Third, reflecting on trust only makes sense when we assume that the environment is uncertain or risky. In our case, we have outlined that the e-credentials market is a prime target of cybercrime but also a potential source for boundless profit-making or surveillance by private or public entities. Trust is an expression of predictability. The statement "I trust the governmental institutions" or "I trust the economic institutions" says nothing necessarily good or bad about them, but rather reflects the notion of trust as a prediction of the behavior of a government or a private sector.

3.3. The relationship between cooperative arrangement types and trust

Having outlined the main constructs, we will now define some statements of relationship. According to Dubin (1978), the nature of a specified relationship depends on a theory's purpose. We seek to develop early substantive (not formal) theory that may help to better explain the choice or dominance of a specific cooperative arrangement in a country's e-credentials market. The relationships we will now formulate are more associative (A may be linked to B) than predictive (when A, then necessarily B). Thus, we make no claims regarding the future or universal or statistical regularities. Nonetheless, we seek to define statements that can be empirically tested and that may shed light on finding the optimal organizational arrangement, given a specific level of citizens' trust.

Building on the findings of the trust index of the Institute of German economy in Cologne (Enste & Grunewald, 2017) and our own inductive inquiry, Fig. 2 shows how trust and cooperative arrangements are related. Two distinct clusters can be identified: first, a group of e-credentials markets where only one state-issued e-ID exists; second, e-credentials markets where different cooperative arrangements prevail. The first group includes Greece, Italy, Poland, Portugal, and Spain. They are all characterized by low or moderate trust in the political institutions, yet the state is the only issuer of e-IDs. This is also true for Ireland, which also has a state e-ID. Ireland, for instance, launched *MyGovID*, which allows citizens to have an online identity. *MyGovID* is built on the Public Services Card and links a citizen's physical

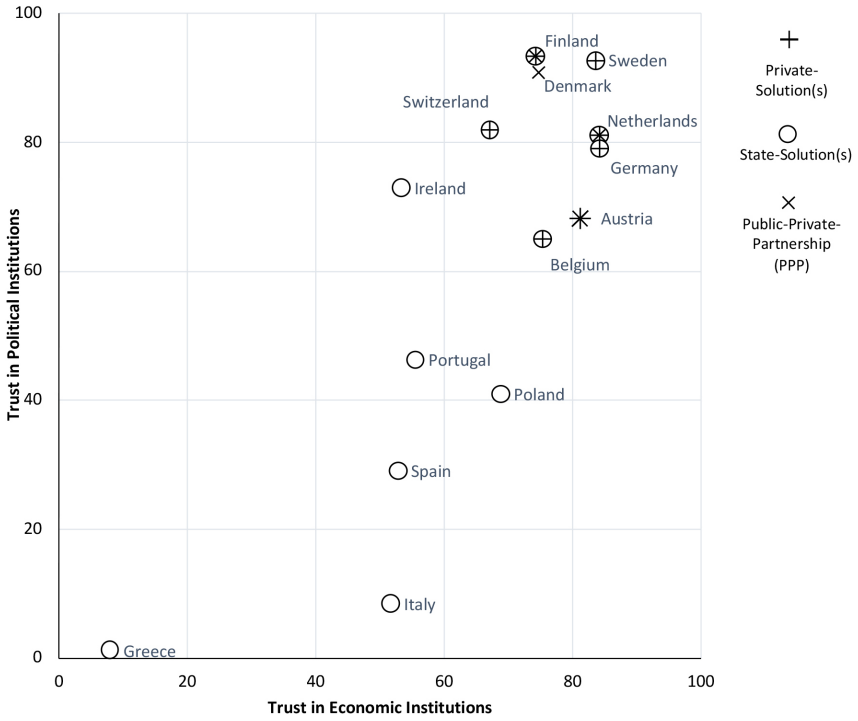

Fig. 2. The relationships between trust and cooperative arrangements.

identity to an online identity. Poland with its *pl.ID* and Portugal both have similar solutions to Ireland. Greece's ERMIS, Italy's SPID, and Spain's DNIe are used not only to access public services, but also to verify users' identity in the private sector.

The second cluster, where trust in the government and the economy are both high, is characterized by the existence of different cooperative arrangement types. This cluster also includes the one outlier, Ireland. Besides Ireland, however, the main characteristic compared to group 1 of e-credentials markets group 1, is that private vendors are somewhat involved in e-ID issuance. Belgium, Germany, Sweden, and Switzerland have both state-driven and private solutions. Belgium strongly relies on its state *beID* solution, which in 2018 was used by approximately five million users for online authentication. Belgium's citizens also have a private identity scheme, *itsme*, which was developed by banks and by telecommunication service providers. Likewise, Germany offers an e-ID based on the German identity card *neuer Personalausweis* ('new identity card'). Further, various e-ID solutions are provided by private vendors. Unlike Belgium and Germany, Sweden primarily relies on e-ID schemes provided by private organizations such as *BankId* and *Telia e-legitimation*. Sweden's government only recently issued its own e-ID initiative, *Freja ID*. Finally, Switzerland, a strongly federalist state, does not yet have a national, state-recognized e-ID; some cantons issue their own e-ID, such as the Cantons of Schaffhausen and city of Zug (Canton of Schaffhausen, 2020; City of Zug, 2020). Other cantons such as Grisons use the e-ID scheme *SwissID*, which is issued by a private consortium of private and semi-public companies.

Interesting constellations can be found in Austria, Denmark, Finland, and the Netherlands, where the e-credentials markets are mainly based on PPPs. Denmark's government approved a new e-ID solution, *MitID*, which will replace the existing *NemID* solution in 2022. The system will be developed in a partnership between the government and Finance Denmark, the Danish banking association. In Austria,

there are two e-ID schemes: the *Bürgerkarte* ('citizen card'), a PPP e-ID solution managed by A Trust GmbH and *e-Identifikation*, a private e-ID alternative issued by banks. Finland and the Netherlands are two e-credentials markets where all e-ID system types exist: PPP-based, public, and private e-ID. Finland has a state-issued e-ID (*FINeID*), which has not achieved widespread use and acceptance among citizens, who prefer the banks' One Time Password (OTP) scheme. This led to the development of a PPP solution called *Tupas* in partnership with the banking sector. *Mobiilivarmenne* is another private e-ID available in Finland. Finally, the Netherlands also has three e-ID schemes: *DigiD*, a state solution used by around 12 million citizens; *eHerkenning*, a PPP between the Ministry of the Interior, Kingdom Relations, and the business community; and *iDIN*, a private system that relies on bank credentials.

3.4. Statement of testable propositions

To enable empirical testing of our observations and claims, we ended our theory development by defining testable propositions:

> ***H1*:** In countries where citizens have high trust in government and economy, there is high likelihood of e-credentials markets with competing cooperative models.

Our analysis revealed that, in countries where citizens generally have high trust in both the government and the economy, there is a higher likelihood of more dynamic and competitive e-credentials markets. This could be explained by the fact that citizens may not have a strong preference or are used to (or even demand) options. Also, governments may have high trust in economic institutions, which increases the likelihood of outsourcing certain activities to or engage with private vendors in PPP constellations. A state official responsible for the e-ID implementation said this about mutual trust:

> "*We have a culture of collaborating. It's really easy to work together and to do it together. It really depends on the collaboration culture in the country. I think that government or private solutions are both possible." (Interviewee, government official)*

Multiple, competing cooperative arrangements seem not to be perceived as a hindrance, but rather as a possibility to experiment or explore which cooperative arrangement may result as the dominant design in a national e-credentials market with a high citizen adoption rate.

> ***H2*:** In countries where citizens have moderate or low trust in the government and the economy, there is a high likelihood of state-driven, monopolistic e-credentials markets emerging.

Paradoxically, our analysis showed that state-driven, monopolistic e-credentials markets emerge in countries where citizens seem to have lower trust in the state than in the economy. However, there is a general mistrust toward both the state and the private sector in cases where only a state solution exists. Pointing to the importance of a long tradition of dealing with citizens' confidential documents, an interviewee noted:

> *"You need to build a lot of trust if you want to convince people to manage their identity. I don't think you would just give it to some company that was founded something over a year ago." (Interviewee, IT service provider)*

Governments have a long tradition of issuing citizens' identity documents. A possible explanation may be that they consider e-ID issuance simply as an extension of existing identity documents and therefore as a sovereign task of the state. Even though citizens may distrust the government more than the economy, in these countries, the state usually acts as market-maker. There may be many alternative explanations

for this phenomenon, including the culturally or historically high influence of the government to take a dominant role in 'sensible' market areas, a reluctance to or ignorance concerning collaborating with businesses, the unavailability of capable and/or trustworthy private vendors, or a risk aversion on the part of private vendors to invest and build an e-ID infrastructure in these countries. Our analysis did not enable us to provide a single coherent answer to this.

Governments play a central role, regardless of whether the trust in them is high or low. Our analysis (see Fig. 2) revealed that even though citizens may trust economic institutions more than a government, this does not necessarily always lead to PPP constellations or to a private e-credentials market. Based on this observation, we hypothesized:

> ***H3*:** In countries where citizens trust the economy more than the government, private e-credentials markets are not more likely to emerge than state-driven, monopolistic e-credentials markets.

Thus, comparatively high trust in the economic institutions is no guarantee that private entities will be involved in issuing these traditionally governmental tasks. There can be multiple reasons, such as legal requirements that hinder the establishment of a private e-credentials market, or simply a lack of interest among private vendors in entering the market owing to unfavorable financial revenues. Interviews indicated that there are also concerns about the data repurposing by private e-ID providers:

> *"e-ID was and is not a technical problem. It was and is only about gaining citizens' trust. In other words, as soon as people believe you're collecting and selling data and are doing profiling or something like that, you're dead." (Interviewee, private e-ID provider)*

Whether or not these or further factors are decisive must be examined closely in each individual case. Our general conclusion is that high trust in the economic institutions seems necessary, but not sufficient for the emergence of an e-credentials market where the state competes with private sector offerings.

4. Conclusion

e-ID development and implementation has been a key issue on the political agenda of many governments, to drive digitalization. e-ID is an important research field, given the growing use of digital identities. In the research, e-ID systems have received much attention not only for single-case analysis (Grönlund, 2010; Hornung & Rossnagel, 2010; Rissanen, 2010) or comparative case analysis (Arora, 2008; Eaton et al., 2018), but also as teaching case studies (Mettler & Guenduez, 2019). Different factors – including privacy considerations and underlying technical aspects (Miyata et al., 2006), historical trajectories and path dependencies (Grönlund, 2010; Kubicek & Noack, 2010), privacy (Strauss, 2011) – have been the focus of previous studies.

Our analysis of different European e-IDs revealed that there are two main e-credentials market types: those where private companies are involved in one form or another in e-ID issuance, and others where they are not. We have sought to theoretically explain the difference in the cooperative arrangements adopted by countries to develop their e-credentials markets. Some of the differences have been subject to comparative case studies. In their cross-case comparative study, Eaton, Hedman, and Medaglia (2018) for instance studied how interactions between the financial and the public sectors influences the emergence of e-ID solutions. Previous studies have conceptualized e-IDs as sociotechnical constructs that have political and economic dimensions (van Dijck & Jacobs, 2019). We built on this work, but focused on trust. With few exceptions (Seltsikas & O'Keefe, 2010; Tolbert & Mossberger, 2006), the importance of trust in this context has received little thought. Our aim in these studies was to provide a theoretical basis for trust's

influence on the preference for cooperative arrangements in e-credentials markets. Specifically, we looked at how trust in economic and the political institutions is linked to a specific cooperation type, i.e. whether e-ID is issued monopolistically, in collaboration with private vendors, or completely outsourced to the market.

Overall, we have shown that there seems to be a correlation between trust in a country's economic and political institutions and the e-ID solutions types available to citizens. Each e-credentials market with fairly high trust in its political and economic institutions typically has a combination of e-ID offerings. Specifically, we could provide evidence that the higher the trust in the political and the economic institutions, the more likely it is that private providers will become involved in e-ID issuance (H1). On the other hand, if trust in both institutions is low, e-ID will likely be issued only by the state (H2). We then developed a third hypothesis and weakened the explanatory power of a key variable, namely that high trust in the economic institutions does not necessarily mean a higher likelihood that cooperative arrangements involving private providers will become the dominant market model (H3).

While trust's role in guiding the choice of organizational arrangement appears to be critical, this has not yet been empirically proven. Our findings have underlined trust's importance in a country's political and economic institutions. We have combined the concept of trust and e-ID at the institutional level. Yet our analysis is by no means conclusive and complete. We have created a good starting point for empirical studies. To better understand trust's role in e-credentials markets, we need more detailed inquiry into distinct trust variables. Such an expanded study may consider additional economic, social, political, and psychological factors that underlie our observations.

We have drawn attention to important discrepancies: In some countries, e-ID is issued by the state, although citizens' trust in the political institutions is low. What does this mean for e-ID usage in these countries? Does the low trust in political institutions also mean that citizens have low trust in the state-issued e-ID? These and other questions open an exciting field for future studies.

From a pragmatic perspective, our hypotheses could be a starting point to critically reflect on the organizational arrangements, specifically whether the chosen organizational arrangement corresponds to the citizens' trust levels. For instance, Poland and Ireland, where trust in political institutions is much lower than in the economy, have government-issued e-IDs. The question arises whether the chosen organizational arrangement is the best or best suited to citizens' trust level. For instance, strong skepticism toward the government could mean that citizens don't perceive a state-issued e-ID as the best option. This also applies to trust in the economy. In cases where trust in the economy is low, a private-issued e-ID could face skepticism among citizens. This can be seen in Switzerland, where the introduction of e-ID at federal level has led to a heated debate about whether the state or private providers should issue e-ID (Mettler & Guenduez, 2019; Guenduez & Schedler, 2019).

These initial results are limited to the e-credentials markets examined in this study and require further investigation to be confirmed. With our strong focus on Europe's e-credentials markets, we cannot fully cover nor ensure the completeness of all the themes and interconnections that are important for understanding trust's role in e-credentials markets. Also, we did not focus on the individual countries' government types, nor on their economic institutions. Further, we did not address whether there were differences between countries in terms of certain arrangements such as PPPs or outsourcing. Yet this was not our goal. We sought to create a theoretical basis for discussion and empirical research. However, collecting and analyzing "different kinds of data from different sources provides a wider range of coverage" of trust's role in e-credentials markets and "increases the robustness of results because findings can be strengthened through triangulation – the cross-validation achieved when different kinds and sources of data converge and are found congruent" (Kaplan & Duchon, 1988, p. 575). It has also helped us to develop an initial understanding of trust's roles in the e-credentials markets we analyzed and helped us to strengthen the theoretical propositions' credibility (Lincoln & Guba, 1985).

References

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53-66. doi: 10.1016/j.ijcip.2014.12.002.

Arora, S. (2008). National e-ID card schemes: A european overview. *Information Security Technical Report*, *13*(2), 46-53. doi: 10.1016/j.istr.2008.08.002.

Belanger, F., & Carter, L. (2008). Trust and risk in e-governmentadoption. *Journal of Strategic Information Systems*, *17*(2), 165-176. doi: 10.1016/j.jsis.2007.12.002.

Blind, P. (2006). *Building trust in government in the twenty-first century: Review of literature and emerging issues*. Paper presented at the 7th Global Forumon ReinventingGovernment, Vienna, Austria.

Bostan, A., Şengül, G., & Karakaya, K.M. (2017). Biometric Verification on e-ID-Card Secure Access Devices: A Case Study on Turkish National e-ID Card Secure Access Device Specifications. *International Journal of Information Security Science*, *6*(4), 87-92.

Canton of Schaffhausen. (2020). Retrieved from https://sh.ch/CMS/Webseite/Kanton-Schaffhausen/Beh-rde/Services/Schaffha user-eID–2077281-DE.html.

Carter, L., & Belanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, *15*(1), 5-25. doi: 10.1111/j.1365-2575.2005.00183.x.

Cheema, G.S. (2010). Building trust in government: An introduction. In G.S. Cheema & P. Vesselin (Eds.), *Building trust in government: Innovations in governance reform in Asia*, New York: United Nations University Press, pp. 1-21.

City of Zug. (2020). Retrieved from https://stadtzugid.zg.ch.

Cordella, A., & Paletti, A. (2019). Government as a platform, orchestration, and public value creation: The italian case. *Government Information Quarterly*, *36*(4), 101409-101409. doi: 10.1016/j.giq.2019.101409.

Dubin, R. (1978). *Theory Building*. New York: Free Press.

Eaton, B., Hedman, J., & Medaglia, R. (2018). Three different ways toskin a cat: Financialization in the emergence of national e-ID solutions. *Journal of Information Technology*, *33*(1), 70-83. doi: 10.1057/s41265-017-0036-8.

Enste, D., & Grunewald, M. (2017). *IW-Vertrauensindex 2017: Vertrauen in Wirtschaft, Politik und Gesellschaft im europäischen Vergleich [IW Trust Index 2017: Trust in Economy, Politics and Society in European Comparison]*. Retrieved from Köln.

Friedman, B., Kahn, P.H., & Howe, D.C. (2000). Trust online. *Communications of the Acm*, *43*(12), 34-40. doi: 10.1145/ 355112.355120.

Gomes de Andrade, N.N., Shara, M., & Martin, A. (2013). ElectronicIdentity in Europe: Legal challenges and future perspectives (e-ID 2020). Retrieved from http://ftp.jrc.es/EURdoc/JRC78200.pdf.

Guenduez, A.A., & Schedler, K. (2019, June 29). Warum wir den Schrittzur elektronischen Identität wagen können. Neue Zürcher Zeitung. Retrieved from: https://www.nzz.ch/meinung/elektronische-identitaet-eine-vertrauens-und-zutrauensde batte-ld.1486345?reduced=true.

Graux, H., Majava, J., & Meyvis, E. (2009). Study on eID interoperabilityfor PEGS – update of country profiles – analysis & assessment report. Retrieved from http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521.

Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). The effect of transparency on trust in government: A cross-national comparative experiment. *Public Administration Review*, *73*(4), 575-586. doi: 10.1111/puar.12047.

Grönlund, A. (2010). Electronic identity management in Sweden: Governance ofa market approach. *Identity in the Information Society*, (3), 195-211. doi: 10.1007/s12394-010-0043-1.

Hengstler, M., Enkel, E., & Duelli, S. (2016). Applied artificialintelligence and trust-The case of autonomous vehicles and medical assistance devices. *Technological Forecasting and Social Change*, *105*, 105-120. doi: 10.1016/j.techfore.2015.12.014.

Hornung, G., & Rossnagel, A. (2010). An ID card for the Internet – The new German ID card with "electronic proof of identity". *Computer Law and Security Review*, *26*(2), 151-157. doi: 10.1016/j.clsr.2009.11.002.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: A case study. *Mis Quarterly*, *12*(4), 571-586. doi: 10.2307/249133.

Komiak, S.Y.X., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *Mis Quarterly*, *30*(4), 941-960.

Kramer, R.M., & Lewicki, R.J. (2010). Repairing and enhancing trust: Approaches to reducing organizational trust deficits. *Academy of Management Annals*, *4*, 245-277. doi: 10.1080/19416520.2010.487403.

Kubicek, H., & Noack, T. (2010). Different Countries-Different Paths Extended Comparison of the Introduction of eIDs in eight European Countries. *Identity in the Information Society*, *3*(1), 235-245.

Lankton, N.K., McKnight, D.H., Wright, R.T., & Thatcher, J.B. (2016). Using expectation disconfirmation theory and polynomial modeling to understand trust in technology. *Information Systems Research*, *27*(1), 197-213. doi: 10.1287/isre.2015.0611.

Lee, J., Kim, H.J., & Ahn, M.J. (2011). The willingness of e-Government service adoption by business users: The role of offline service quality andtrust in technology. *Government Information Quarterly*, *28*(2), 222-230.

Lentner, G.M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government: People, Process and Policy*, *10*(1), 8-25.

Lincoln, Y.S., & Guba, E.G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage.
Llewellyn, S., Brookes, S., & Mahon, A. (Eds.). (2013). *Trust and Confidence in Government and Public Services*. London: Routledge.
Luhmann, N. (1979). *Trust and Power*. Chichester, U.K: Wiley.
Luo, X., Li, H., Zhang, J., & Shim, J.P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance ofemerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, *49*(2), 222-234. doi: 10.1016/j.dss.2010.02.008.
McKnight, D.H., & Chervany, N.L. (1996). *The meanings of trust*. Technical report. Universityof Minnesota Management Information Systems Research Center.
McKnight, D.H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359. doi: 10.1287/isre.13.3.334.81.
Melin, U., Axelsson, K., & Söderstrïm, F. (2016). Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective. *Transforming Government: People, Process and Policy*, *10*(1), 72-98.
Mettler, T., & Guenduez, A.A. (2019). From SuisseID to SwissID: Overcoming the key challenges in Switzerland's e-credential market. *Paper presented at the 40th International Conference on Information Systems, Munich*.
Mir, U.B., Kar, A.K., Dwivedi, Y.K., Gupta, M., & Sharma, R. (2019). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly*, *37*(2), 101442.
Miyata, T., Koga, Y., Madsen, P., Adachi, S., Tsuchiya, Y., Sakamoto, Y., & Takahashi, K. (2006). A survey on identity management protocols and standards. *Ieice Transactions on Information and Systems*, *E89D*(1), 112-123. doi: 10.1093/ietisy/e89-d.1.112.
Morgeson, F.V., VanAmburg, D., & Mithas, S. (2011). Misplaced Trust? Exploring the Structure of the E-Government-Citizen Trust Relationship. *Journal of Public Administration Research and Theory*, *21*(2), 257-283. doi: 10.1093/jopart/muq006.
Morse, J.M. (2010). Simultaneous and sequential qualitative mixed method designs. *Qualitative Inquiry*, *16*(6), 483-491. doi: 10.1177/1077800410364741.
Muñoz-Cañavate, A., & Hípola, P. (2011). Electronic administration in Spain: From its beginnings to the present. *Government Information Quarterly*, *28*(1), 74-90.
OECD. (2019). *OECD Business and Finance Outlook 2019: Strengthening Trust in Business*. Retrieved from Paris.
Popper, K. (1934). *Logik der Forschung [The Logic of Scientific Discovery]*. Vienna: Springer.
Putnam, R.D. (1993). *Making Democracy Work. Civic Traditions in Modern Italy*. Princeton: Princeton University Press.
Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society*, *3*, 175-194.
Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393-404. doi: 10.5465/amr.1998.926617.
Sabherwal, R., & King, W.R. (1991). Towards a theory of information resources of strategic use An inductive approach. *Information & Management*, *20*(3), 191-212. doi: 10.1016/0378-7206(91)90055-7.
Sangnier, M. (2013). Does trust favor macroeconomic stability? *Journal of Comparative Economics*, *41*(3), 653-668. doi: 10.1016/j.jce.2012.10.002.
Seltsikas, P., & O'Keefe, R.M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value. *European Journal of Information Systems*, *19*(1), 93-103. doi: 10.1057/ejis.2009.51.
Sicari, S., Rizzardi, A., Grieco, L.A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. doi: 10.1016/j.comnet.2014.11.008.
Simpson, J.A. (2007). Psychological foundations of trust. *Current Directions in Psychological Science*, *16*(5), 264-268. doi: 10.1111/j.1467-8721.2007.00517.x.
Spagnoletti, P., Me, G., Ceci, F., & Prencipe, A. (2019). Securing national e-ID infrastructures: Tor networks as a source of threats. In *Organizing for the Digital World*, Cham: Springer, pp. 105-119.
Strauss, S. (2011). The Limits of Control – (Governmental) Identity Management from a Privacy Perspective. *Privacy and Identity Management for Life*, *352*, 206-218.
Teo, T.S.H., Srivastava, S.C., & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of Management Information Systems*, *25*(3), 99-131. doi: 10.2753/mis0742-1222250303.
Thomas, D.R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, *27*(2), 237-246. doi: 10.1177/1098214005283748.
Tolbert, C.J., & Mossberger, K. (2006). The effects of e-government on trust and confidence in government. *Public Administration Review*, *66*(3), 354-369.
van Dijck, J., & Jacobs, B. (2019). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, *22*(5), 896-914. doi: 10.1177/1461444819872537.
Wang, Y.D., & Emurian, H.H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105-125. doi: 10.1016/j.chb.2003.11.008.
Webster, J., & Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Mis Quarterly*, *26*(2), XIII-XXIII.

Welch, E.W., Hinnant, C.C., & Moon, M.J. (2005). Linking citizen satisfaction with e-government and trust in government. *Journal of Public Administration Research and Theory*, *15*(3), 371-391. doi: 10.1093/jopart/mui02l.

Whetten, D.A. (1989). What constitutes a theoretical contribution? *Academy of Management Review*, *14*(4), 490-495. doi: 10.2307/258554.

Whitley, E.A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, *23*(1), 17-35. doi: 10.1057/ejis.2013.34.

Wihlborg, E. (2013). Secure electronic identification (eID) in the intersection of politics and technology. *International Journal of Electronic Governance*, *6*(2), 143-151.